US Army Corps
of Engineers

Electronic Signature Users Guide

Version 2.0

CEFMS

Corps of Engineers Financial Management System

March 30, 1998
Revised January 4, 2000

FOREWORD

The CEFMS Electronic Signature capability is limited to valid CEFMS users who have been granted authorization in the Access Control Table. To perform these capabilities, an individual must be assigned a **smartcard**. There are grave responsibilities that come with the issuance and receipt of smartcards. Refer to Appendix A of this document for a list of smartcard holder’s responsibilities, along with signature requirements acknowledging that as a smartcard holder you have read and understand these responsibilities. Appendix B provides similar signature requirements for smartcard approvers.

ELECTRONIC SIGNATURE USERS GUIDE

TABLE OF CONTENTS

LIST OF FIGURES

ELECTRONIC SIGNATURE USERS GUIDE

TABLE OF CONTENTS (CONT.)

PAGE

APPENDICES

SECTION 1.0 GENERAL

1.1 <u>Introduction</u>.

The Corps of Engineers Financial Management System (CEFMS) provides the capability to electronically sign documents. The electronic signature generated by the system is a replacement for a handwritten signature. An electronic signature will provide assurance that a document was signed by an authorized person and that the document was not altered after it was signed. Hardcopy documents can be altered without detection and handwritten signatures can be forged. With electronic signatures, these alterations will be detected. Electronic Signatures will reduce the amount of paper that must be routed. Documents can be reviewed on screen and signatures verified using the Electronic Signature System (ESS). The following paragraphs provide information that a user or security administrator should have in using the system.

1.2 <u>Definitions</u>.

The following terms are commonly used when referring to the electronic signature system.

1.2.1 <u>ARGUS 300 Adapter Board</u> - a board installed in a PC which performs the functions of the electronic signature system.

1.2.2 <u>CEFMS Database Administrator (DBA)</u> - an individual providing technical support, including enforcing the policies and standards set by the data administrator for the database. In addition to providing maintenance, the DBA coordinates with other computer operations technicians, system developers, vendors, and users.

1.2.3 <u>Central Security Officer (cSO)</u> - a person at a regional center responsible for maintaining the Key Translation Center (KTC) of the ESS. There will be two cSOs at each regional center with each having a backup.

1.2.4 <u>Cryptographic Keys</u> - keys that are stored on the card or generated by the PC Adapter Board and used in the electronic signature process.

1.2.5 <u>Data Administrator (DA)</u> - the individual responsible for the life-cycle management of the information describing the functions, operations, and structure of the organization’s databases. These responsibilities include prescribing policies and standards, planning, coordinating, resolving conflicts, designing logical databases, and controlling security. The DA also ensures that life-cycle planning includes on-line retention issues as well as archival criteria and methods.

1.2.6 <u>Database</u> - a generalized, integrated collection of interrelated data, organized according to a plan to satisfy the data requirements of all applications which use it.

1.2.7 District Security Officer (dSO) - a person responsible for issuing smartcards, Personal Identification Numbers (PINs), and performing other Electronic Signature management functions. There are two primary dSOs designated dSO1 and dSO2. Primary dSOs have at least one (but no more than two) backup designated dSOb1 and dSOb2.

1.2.8 Electronic Signature Drivers/Software - software to interface CEFMS and other applications with the PC Adapter Board.

1.2.9 Key Translation Center (KTC) - a central database containing all the Users of the Electronic Signature System (ESS), i.e., cSOs, dSOs, SAs, and Users. This database is accessed when verifying the signature of a user. There will be two regional centers located at Vicksburg, MS and Portland, Oregon. Each will have two KTCs and will serve as backups for each other.

1.2.10 Message Authentication Code (MAC) - a combination of characters which represents the electronic signature. The MAC is generated using the data being signed and the User's and SA's cryptographic keys.

1.2.11 PC Adapter Board - a board installed in a PC which performs the functions of the ESS.

1.2.12 Personal Identification Number (PIN) - a randomly generated pronounceable password issued to a cSO, dSO, SA, or User which is required in order to use the ESS. Upon entering CEFMS, the application prompts the cSO, dSO, SA or User to insert their smartcard into the smartcard reader and then prompts for their PIN.

1.2.13 Security Administrator (SA) - an employee issued a card who will be responsible for initialization of a PC Adapter Board so that users can sign documents. SAs who initialize PC Adapter Boards in PCs used in the disbursing functions and the user signing the checks will be held liable for fraudulent transactions. SAs will not be held liable for fraudulent or erroneous transactions signed for by Users with signature authority for functions outside of disbursing.

1.2.14 Smartcard (card) - a card, similar in size and shape to an automated teller card or credit card. A smartcard is issued to each authorized cSO, dSO, SA, or User to gain access to the ESS. The smartcard contains a microprocessor chip that actually stores data and performs calculations. Each card has its own serial number for identification. The smartcard is commonly referred to as a signature card.

1.2.15 Smartcard Approver - a person responsible for approving an employee’s request for a smartcard. The Smartcard Approver ensures the employee is authorized by the Laboratory or Support Staff Chief to obtain a smartcard. Upon verification, the request is approved and electronically sent to the dSOs.

1.2.16 **Smartcard Reader** - a device connected to the PC adapter board which reads data stored on the smartcard and passes it securely to the PC adapter board.

1.2.17 **User** - an employee issued a smartcard and responsible for signing documents. Users who electronically sign documents accept the same responsibility as when signing documents by hand.

1.3 Hardware/Software Requirements.

To electronically sign documents, a smartcard user logs onto CEFMS on a computer equipped with the Electronic Signature hardware and software. The basic computer requirements include:

- PC with AT(ISA) Bus 80286, 80386, or 80486 CPU with EGA or VGA monitor and appropriate card. **NOTE:** The Electronic Signature will not work on a Macintosh or an IBM PS/2 computer. Electronic signature may be used with a notebook computer with the Signet device.

- 640 KB RAM; but recommend at least 2.5 additional MB RAM if other software packages will be run on your PC.

- 300 KB hard disk storage; but recommend at least 5 MB hard disk storage if other software applications will be run on your PC.

- DOS 5.0 Or higher if possible.

- 1 serial port.

- 3COM 3c503 Ethernet card if on an Ethernet Lan.

- Capability to access the CEFMS database via LAN connection or modem.

- PC Adapter Board.

- Smartcard Reader.

- Electronic Signature Software.

- Activated Smartcard.

- Personal Identification Number (PIN).

SECTION 2.0 SECURITY PROCEDURES

2.1 Smartcard Security.

When receiving a card and PIN, it is very important to follow the security procedures listed below.

2.1.1 Always keep the card in a safe place when it is not being used. A wallet or a locked drawer is the best place to keep the card.

2.1.2 Sign the PIN envelope before opening to validate that it has not been tampered with prior to receipt.

2.1.3 Return the top sheet of the envelope to the dSO issuing the password.

2.1.4 Memorize the PIN then destroy the second sheet of the envelope. Do not throw it away without shredding the document first.

2.1.5 Do not write the PIN down or give it to another User.

2.1.6 If the PIN is revealed to another User, immediately contact the dSO for a new card. If the card is lost or stolen, immediately contact the dSO. The dSO will deactivate the card so that it can no longer be used. A new card and PIN will be issued.

2.1.7 A lost card or compromised PIN is a serious security issue since the User can be held responsible for transactions authorized with the missing or compromised card.

CONTACT THE dSO *IMMEDIATELY* IF A CARD IS LOST OR PIN COMPROMISED.

2.2 Deactivate Smartcard Due to Employment Termination.

Smartcards will be deactivated when a user leaves an organization. The card must be returned to the dSOs so it can be deactivated to prevent the user from signing any additional messages. The flag in the database will be set to indicate that although the user is no longer active, the signatures generated by the user may still be validated.

2.3 Compromised PIN.

Smartcards will be deactivated when a PIN is compromised or the user suspects a PIN is compromised. The smartcard must be promptly returned to the dSOs. The user is not deleted from the database so that signatures generated by the user may still be used to verify messages previously signed by the user. The user will receive a new smartcard and PIN.

2.4 Lost Smartcard.

Smartcards will be deactivated when a card is lost. The dSOs must be notified immediately that a card was lost. The database will be updated to set the flag to indicate that although the card is no longer active, the signatures previously generated by the user may still be verified. The database will be updated with the date a smartcard is deactivated. Any signature generated after this date may not be verified. The user will receive a new smartcard and PIN.

2.5 Security Violations.

2.5.1 If a user sees or knows of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual's supervisor for appropriate disciplinary action.

2.5.2 If a user finds an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If you cannot log them off, remove the smartcard and take to the individual's supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

2.5.3 If you find a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

2.5.4 If you find a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.

SECTION 3.0 OPERATING PROCEDURES

3.1 Requesting a Smartcard.

Requests for a smartcard and PIN must be made through CEFMS. The request is approved by an authorized person, who then forwards the request to the dSOs. The dSOs assign a card and then issue the card and PIN to the requestor.

3.1.1 To request a smartcard, a valid CEFMS user ID and password are required. After receiving a userid and password, follow the steps listed below in order to request and receive a smartcard:

- Login to the system where the CEFMS database resides.

- Enter the command to execute CEFMS.

- From the CEFMS Main Menu, select option 7 - **ELECTRONIC SIGNATURE FUNCTIONS.**

- From the Electronic Signature Menu, select option 3 - **REQUEST SMARTCARDS.** This option will display screen 15.1, Request Electronic Signature Smartcard.

- Press **<F9>** to request card and then enter the card type: **U** for User Card, **S** for Security Administrator Card, **D** for Security Officer Card.

- **<PGDN>** to view the request information and check the request status.

3.1.2 A user may only make one request at a time. If a user has a smartcard, that card must be deactivated by the dSOs before another card request can be made.

3.1.3 The request will be electronically forwarded to a Smartcard Approver, who must electronically approve the request before a smartcard can be issued. Reference Appendix B for Smartcard Approvers duties.

3.1.4 Once the request is approved, the dSOs will assign a smartcard. A dSO will notify the requestor as to when and where the card and PIN can be obtained. If the card and PIN is to be received in person, the dSOs will activate the smartcard and present the smartcard and PIN envelope to the user. The user must then sign and date the PIN envelope and leave the header sheet with the dSOs. (If the requestor is at a remote site, a dSO will mail the PIN envelope first. The smartcard will not be activated and mailed until the PIN envelope is signed and the header sheet returned to the dSOs.)

3.2 Issuing of Smartcards.

If a user appears in person to receive a smartcard:

3.2.1 A valid driver license or Civilian ID card may be required to verify identification.

3.2.2 The individual will be given a copy of the Electronic Signature Users Guide. The user must read, sign, and date the Smartcard Holders Responsibilities Form before receiving a smartcard and PIN. A copy of the signed signature page will be provided to the user.

3.2.3 After verifying the person's identity, the dSOs will activate the smartcard and issue the smartcard and PIN to the employee.

- If the smartcard being issued is for a User, dSO1 will issue the smartcard and dSO2 will issue the User PIN envelope.

- If the smartcard being issued is for an SA, dSO2 will issue the smartcard and dSO1 will issue the SA PIN envelope.

3.2.4 The individual will check the PIN envelope to detect tampering. If none is found, the user will sign the top portion of the envelope, tear it off, and return to the issuing dSO. The dSO will file the signed top portion.

3.2.5 The bottom portion containing the smartcard holer's unique PIN (i.e., password) is kept by the individual.

3.3 Remote Assignment and Issuing of Smartcards.

If a user is remotely located and cannot receive his/her card in person:

3.3.1 If the smartcard request is approved by the Smartcard Approver, the dSOs will assign a smartcard through the DSO CARD ASSIGNMENT SCREEN.

3.3.2 The requestor will be mailed the smartcard by **Certified Mail - Return Receipt Requested**.

3.3.3 When you receive the smartcard, sign for the Certified Mail and call the issuing dSO to let him/her know you have received your smartcard. If you do not receive your smartcard in a reasonable amount of time or if the smartcard is damaged, notify the dSO so that appropriate action can be taken.

3.3.4 Upon confirmation that you have the smartcard, the dSO will mail the PIN envelope by **Certified Mail - Return Receipt Requested**.

3.3.5 When received, sign for the mail. Examine the PIN envelope for tampering. If okay, sign the top portion of the PIN envelope and tear it open. The bottom portion contains your PIN and serial number of your assigned card. **Memorize the PIN and destroy the bottom portion** of the envelope by shredding or burning. Any hard copy of a PIN must be kept in your physical possession or secured in a locked cabinet, drawer, or container accessible only by you.

3.3.6 Return the top portion of the PIN envelope to the issuing dSO by **U.S. Postal Service - Regular Mail, First Class**.

3.3.7 Call the issuing dSO to acknowledge receipt of the PIN envelope.

3.3.8 Upon confirmation that you have received the PIN envelope, the appropriate dSO will activate the smartcard.

3.4 Expiration of Smartcards.

All user and SA cards will expire within three years from the date of activation except users performing disbursing and dSO functions; and those cards will expire in one (1) year. The one (1) year expiration occurs when the Access Control authorization for receipt voucher audit (rv_audit_ind) or receipt voucher certification (rv_cert_ind) or disbursing authority (disb_auth) or disbursing officer (disb_officer_ind) or district security officer (dist_sec_ofcr_ind) or travel settlement authority (trv_setl_auth_ind) = ’Y’. Users will be given the first warning message 30 days before the card will expire. The user may request a new card even though the current card is not deactivated. However, the old card must be turned in before the dSOs can activate the new card. **REQUEST A NEW CARD AS SOON AS** the warning message is given! Expired cards cannot access the ESS.

3.5 General Operating Procedures.

3.5.1 The card types are designed for either a User or a Security Administrator (SA). An SA can also be a User; but a User cannot be the designated SA and user on a PC at the same time.

3.5.2 The SA must initialize the PC adapter board to be used for electronic signatures. After the SA has initialized the board, any number of Users can use the Electronic Signature System to sign documents.

3.5.3 Cards must be inserted into the card reader correctly. The LITRONIC logo should face **down**. With thumb on the arrow, insert into the card reader.

3.5.4 CEFMS will then prompt for a PIN. When entering a PIN, the CAPS LOCK key should be **off**. The PIN will be in **lower case.**

3.6 Security Administrator (SA) Operating Procedures.

3.6.1 If a board has not been previously initialized by an SA, a screen will appear when entering CEFMS which prompts the SA to enter the card and then the PIN.

3.6.2 The SA will be given four tries to enter the correct PIN after which CEFMS will log you out. After nine consecutive incorrect PINs, the card will be locked and the dSO will have to unlock the card.

3.7 User Operating Procedures.

Once the SA has initialized the PC Adapter Board, the User will be prompted to insert the card and enter the PIN. The User will follow the procedure in **paragraphs 3.3.3** and **3.3.4**. The User will be given four tries to enter the correct PIN after which CEFMS will log you out. After nine consecutive incorrect PINs, the card will be locked.

3.7.1 After a successful log on, do not remove your card until you exit from CEFMS. If the card is removed before exiting CEFMS, the card will be locked. Users may unlock their own card when logging back into CEFMS.

3.7.2 When entering CEFMS, several errors may occur that will prevent the User from using the electronic signature capability. If errors occur while using the electronic signature capability, write down the error code and contact your site's CEFMS POC for resolution of the problem.

3.7.3 If a signature does not verify on a document, a message will appear on the screen. This indicates that the document has been altered in some way and the alteration must be resolved in order to continue. Contact the originator of the document or your site's CEFMS point of contact to resolve the problem.

3.7.4 After entering CEFMS, an error message may appear during the verification or signing of a document. If an error occurs, write down the error code that appeared and contact your site's CEFMS POC for resolution of the problem.

3.8 District Security Officer (dSO) Operating Procedures.

Reference Appendix C for the functions, responsibilities, and operating procedures of the dSO.

3.9 Access Control Functions Which Require Electronic Signature.

Electronic Signature will be the means used to identify the authenticator of information and to verify that critical data on a document has not been altered. The only required users of Electronic Signature are those who perform level III security functions, i.e., those where actions/approvals lead to an obligation, collection, or disbursement of government funds.

3.9.1 The immediate supervisor of each employee requiring access to the CEFMS database may be tasked to submit the Request For CEFMS Access Form. This form will be submitted to the CEFMS DataBase Administrator. The functions checked on the form provide information for the CEFMS DBA to grant the user access and authorization to control the activities they will be able to perform, including the need for electronic signature capability. Figure 3-1 depicts a sample CEFMS Access Form.

3.9.2 The CEFMS DBA will ensure that the appropriate Smartcard Approver receives the names of individuals needing a smartcard based on authorizations granted in the CEFMS Access Control Table. An asterisk indicates those authorizations which require electronic signature capability. To obtain a more detailed understanding of the functions capabilities which are assigned through the CEFMS Access Control Table, reference the CEFMS Access Control (Authorizations Cross Referenced To Functionalities) document.

REQUEST FOR CEFMS ACCESS FORM

NAME: ______________________________ USERID:___________ PHONE: __________________
SUPERVISOR'S APPROVAL: ________________________________ DATE: _____/_____/______

Check The Desired Access (*Requires Esig Capability):

|*| ACCPT CUST ORD
|_| ACCRUAL AUTHORITY
|_| ACPERS
|_| ADJUST WAREHOUSE INVENTORY
|_| AGENCY RATE AUTHORITY
|_| APPROP EXP AUTHORITY REQUEST
|_| APPROP EXP AUTHORITY APPROVAL
|_| APPROVE ADJUST WAREHOUSE INVENTORY
|*| APRV PR&C
|_| ASSET BATCH IND
|_| ASSET MANAGER AUTHORITY
|*| AUTHORIZED COLLECTOR
|_| AUTHORIZED PROPERTY OFFICER
|*| AUTHORIZED RECEIVER
|_| BUDGET APPROVAL AUTHORITY
|_| BUDGET FORMULATION LEVEL
|*| CERT PR&C
|*| CERTIFY GOV'T TRAINING BILLS AUTH
|*| CERTIFY TRAINING TFO's AUTHORITY
|*| COMMERCIAL TRANSPORTATION AUTH
|*| CONVERSION AUTHORITY
|_| COST SHARE CONTROL IND
|_| COST SHARE ESCROW/LOC AUTH
|_| COST SHARE RECORD EARNINGS IND
|_| COST SHARE RECORD IN-KIND IND
|_| COST TRANSFER
|_| CUPBOARD STOCK TRANSFER IND
|_| CUSTOMER ORDER ROLLOVERS
|_| DATA MGR ESIG FAIL RESOLUTION AUTH IND
|*| DISBURSING AUTHORIZATION
|*| DISBURSING/DEPUTY DISBURSING OFFICER
|*| DISBURSING SCRTY ADMIN AUTH
|*| DISTRICT SECURITY OFFICER
|_| ELECTRONIC FUNDS TRANSFER AUTH IND
|*| ENG 93 C.O.R. APPRV
|*| ENG 93 P.M. APPRV
|*| FINAN APRV
|_| FOREIGN CURRENCY REVALUATION AUTH IND
|*| FUND OVRD
|_| FUNDING ACCOUNT IND
|_| FUNDING ACCOUNT OVERHEAD IND
|_| FUNDING CREATOR
|_| GENERAL LEDGER JOURNAL AUTHORITY
|_| GENERATE CUSTOMER ORDER BILLS
|_| GENERATE FACILITY BILLINGS
|_| GENERATE INVENTORY BILLINGS
|_| GENERATE PLANT RENTAL BILLINGS
|*| GOVERNMENT ORDER ACCEPTOR
|_| IATS INTERFACE AUTHORITY
|*| IMPREST FUND CASHIER
|_| INCOME TRNS IND
|_| INTRA CORPS TRANSFER AUTHORITY
|*| INVOICE CREATOR
|_| JOB ORDER FUNDING CREATOR
|_| LABOR CERTIFICATION AUTHORITY
|_| LABOR DISTRIBUTION AUTHORITY
|_| LEDGER POSTING AUTH
|_| MULTI-PURPOSE POWER AUTH IND
|*| OBLIGATE TRAINING REQUEST AUTHORITY
|*| OBLIGATION APPROVER
|_| ORGANIZATION RATE AUTHORITY
|_| ORIG PR&C
|*| OTHER PURCHASES APPROVER IND
|*| OTHER PURCHASES CERTIFIER IND
|*| OTHER PURCHASES OBLIGATOR IND
|*| PCS TRAVEL AUTHORITY
|_| PERIOD CONTROL
|_| PLANT RENTAL RATE AUTHORITY
|_| PLO
|_| PRC AUTHORIZED ASSIGNER
|_| PROCESS LONG TERM REVENUE
|*| PROCESS RECEIPT VOUCHER
|*| PROCESS TRANS. BY OTHERS (TBO's)
|*| RECEIPT VOUCHER AUDITOR
|*| RECEIPT VOUCHER CERTIFIER
|_| RELEASE OF CLAIMS AUTHORITY
|_| REORG AUTH IND
|_| REPORT ACCESS LEVEL
|_| REPORT SUBMISSION IND
|_| REPORT VIEW LEVEL
|_| RESOURCE PLANS/ESTIMATES APPROVER
|_| REVENUE GENERATING AGREEMENT MAIL CODE
|_| REVERSE ACCRUALS AUTH
|_| S&A COST TRANSFER IND
|_| S&A MEMO PLACEMENT AUTH IND
|*| S&A OBLIGATION AUTH
|_| S&A PROCESS AUTHORITY
|_| S&A TRANSFER TO UFC IND
|_| SAACONS INTERFACE AUTH IND
|_| SHOP/FACILITY RATE AUTHORITY
|*| SMARTCARD REQUEST APPRV
|_| SPECIFIC EXPENDITURE AUTHORITY IND
|*| SUPERVISOR
|_| TECH APRV
|_| TIMEKEEPER
|_| TRAINING REQUEST APPROVAL AUTHORITY
|*| TRAV VOUCHER/L.D. PHONE REVIEWER AUTH
|*| TRAVEL ADVANCE AUTH IND
|_| TRAVEL APPROVING OFFICIAL
|*| TRAVEL AUTHENTICATING OFFICIAL
|_| TRAVEL REQUESTING OFFICIAL
|*| TRAVEL SETTLEMENT CERTIFY IND
|_| TRAVEL SETTLEMENT CREATE IND
|_| TRAVELERS CHECKS AUTH IND
|_| USER STATUS
|*| VENDOR APPROVAL AUTHORITY
|_| WAREHOUSE BURDEN RATE AUTHORITY
|_| WAREHOUSE STOCK RECORD AUTHORITY
|_| YEAR END CLOSINGS IND

Figure 3-1

3.10 Error Messages.

3.10.1 When entering CEFMS, several errors may occur that will prevent a smartcard holder from using the Electronic Signature capability. The user will be able to continue, but will not be able to verify any signatures electronically or electronically "sign" a document. If an error occurs, write down the error code and contact your site's CEFMS POC.

3.10.2 The following is a general list of error codes and messages to aid in the diagnosis of error conditions.

ERROR CODE	EXPLANATION OF ERROR
0	ElecSig: Success
1	Cannot get terminal characteristics
2	Cannot stat terminal driver
3	Cannot find interface program
4	Transmit of data failed
5	Unspecified ESIGMGR failure
6	Cannot set TTY to raw model
7	Cannot change TTY model
8	Network load to high, can't communicate with / RCV communication timeout
9	Cannot find interface program
10	SA logon terminated voluntarily
11	User card is locked, contact security office
12	Translate keys not available
13	SA logon failed
14	User logon failed
15	No response from PC
16	Error getting host name
20	Security adaptor missing
21	Data integrity failed, contact document originator
22	Security breach
23	User card removed
24	ESIGMGR not responding, esig impossible
25	Service failed
26	Host failed
27	Proto failed
28	Read socket create
29	Read socket bind
30	Read socket name
31	Read socket listen

ERROR CODE	EXPLANATION OF ERROR
32	Write socket create
33	Write socket connect
34	Write failed
35	Request for new cards failed
36	Inactive user card used
37	Inactive SA card used
60	Header MAC received does not match computed
90	Password must be at least 8 chars
91	Password entered incorrectly
92	SO logon voluntarily terminated
93	Esig changed
94	Cannot open connection
95	ESIGISR not loaded
97	No free key record in card
98	Key ID not found
99	No free key entry in adaptor
100	Key record's card address is zero
101	Invalid active key number
102	Key parity error
103	Invalid key type
104	Key management not initialized
105	Invalid card header
106	Invalid function for link model
107	Privilege violation
108	Unused key record in card
109	Invalid key record in card
110	Suspended key record in card
111	Key entry in use
112	No such key entry
113	Key entry not in use
114	No key encrypting key active
115	Key with given ID already in key store
116	Invalid key type for key function given
117	Key already active
118	Key entry checksum failure
119	Invalid password
120	Attempt to decrement key counter
121	Incompatible key sizes
123	Key XOR violation
124	Key encryption violation
125	Key is discontinued

ERROR CODE	EXPLANATION OF ERROR
126	Key checkword failure
127	Link authentication failure
128	OU mac after deactivation date
129	OU mac after lost date
130	OS mac after deactivation date
131	OS mac after lost date
132	RU mac after deactivation date
133	RU mac after lost date
134	RS mac after deactivation date
135	RS mac after lost date
150	Field format error
151	Nested delimiters
152	Unmatched delimiters
153	Duplicate MID, MAC, or date field
154	No date field
155	No MAC field
156	No MID field
157	Accept failed
158	Read failed
159	SO not logged in
160	No data to MAC in storage
161	No MAC to verify (esig not mandatory)
162	Initialize CEFMS failed (esig not mandatory)
163	No MAC to verify (esig mandatory)
164	Initialize CEFMS failed (esig mandatory)
165	DSO1 logon failed
166	DSO2 logon failed
167	Must use ESIGMGR, not VCOM menu - emulation flag error
220	Dirty line
221	Checksum failed
225	No such card
226	Card already active
227	Cryptoperiod has expired
228	User cryptoperiod has expired
229	SA cryptoperiod has expired
230	Orig User cryptoperiod has expired
231	Orig SA cryptoperiod has expired
234	Bad Org SAID
235	Bad Org UserID
236	Bad RCV SAID
237	Bad RCV UserID

ERROR CODE	EXPLANATION OF ERROR
238	Counter for this instance is not stored at.KMS
239	Counter for this instance is out of sync with KMS counter
240	Could not connect to ORACLE to retrieve counter
240	User logon terminated voluntarily
241	Could not SELECT counter field from FOA -UNIQUE table
246	User pressed "skip" key
247	User pressed "quit" key
248	Your ElecSig driver is the wrong version. Contact system administrator
249	dSO2 card not in receptacle
251	Oracle error - 1002, 1403 nothing return from select (treat this as a warning)
255	Driver initialization failed, no elecsig capability
255	Cannot verify, document was not electronically signed
999	Unknown error

APPENDIX A

SMARTCARD HOLDER’S RESPONSIBILITIES

APPENDIX A

SMARTCARD HOLDER'S RESPONSIBILITIES

If there are any questions concerning your responsibilities as a smartcard holder, please ask a District Security Officer (dSO) for an explanation. If there are no questions, sign and date this form; make a copy of the signed form for your records and return the original to the issuing dSO.

1. <u>RECEIVING YOUR SMARTCARD</u>.

a. If a user appears in person to receive a smartcard:

(1) A valid driver license or Civilian ID card may be required to verify identification.

(2) The individual will be given a copy of the Electronic Signature Users Guide. The user must read, sign, and date the Smartcard Holders Responsibilities Form before receiving a smartcard and PIN. A copy of the signed signature page will be provided to the user.

(3) After verifying the person's identity, the dSOs will activate the smartcard and issue the smartcard and PIN to the employee.

- If the smartcard being issued is for a User, dSO1 will issue the smartcard and dSO2 will issue the User PIN envelope.

- If the smartcard being issued is for an SA, dSO2 will issue the smartcard and dSO1 will issue the SA PIN envelope.

(4) The individual will check the PIN envelope to detect tampering. If none is found, the user will sign the top portion of the envelope, tear it off, and return to the issuing dSO. The dSO will file the signed top portion.

(5) The bottom portion containing the smartcard holer's unique PIN (i.e., password) is kept by the individual.

b. If a user is remotely located and cannot receive his/her card in person:

(1) If the smartcard request is approved by the Smartcard Approver, the dSOs will assign a smartcard through the DSO CARD ASSIGNMENT SCREEN.

(2) The requestor will be mailed the smartcard by **Certified Mail - Return Receipt Requested**.

(3) When you receive the smartcard, sign for the Certified Mail and call the issuing dSO to let him/her know you have received your smartcard. If you do not receive your smartcard in a reasonable amount of time or if the smartcard is damaged, notify the dSO so that appropriate action can be taken.

(4) Upon confirmation that you have the smartcard, the dSO will mail the PIN envelope by **Certified Mail - Return Receipt Requested**.

(5) When received, sign for the mail. Examine the PIN envelope for tampering. If okay, sign the top portion of the PIN envelope and tear it open. The bottom portion contains your PIN and serial number of your assigned card. **Memorize the PIN and destroy the bottom portion** of the envelope by shredding or burning. Any hard copy of a PIN must be kept in your physical possession or secured in a locked cabinet, drawer, or container accessible only by you.

(6) Return the top portion of the PIN envelope to the issuing dSO by **U.S. Postal Service - Regular Mail, First Class**.

(7) Call the issuing dSO to acknowledge receipt of the PIN envelope.

(8) Upon confirmation that you have received the PIN envelope, the appropriate dSO will activate the smartcard.

2. SMARTCARD and PIN USAGE. Your smartcard is logged on when entering CEFMS and logged off with a normal termination. **DO NOT LEAVE THE COMPUTER UNTIL YOU HAVE COMPLETED YOUR SESSION.**

a. When exiting CEFMS, DO NOT remove your smartcard until you see the message "USER CARD IS BEING LOGGED OFF". Then you may remove your smartcard. If you remove your smartcard prior to this message, it will become locked.

b. If your smartcard becomes locked, enter the CEFMS database again. A screen will prompt you to insert your smartcard and enter your PIN. If done properly, this procedure will unlock your smartcard, and allow you to successfully log into CEFMS.

3. SECURITY OF THE SMARTCARD AND PIN. Memorize your PIN. DO NOT write it down (especially on the smartcard) or share with others.

   a. When not in use, keep your smartcard in your possession, preferably a wallet or purse, or in a locked cabinet, drawer, or container accessible only by you. DO NOT LEAVE YOUR WALLET OR PURSE UNSECURED OR UNATTENDED BY YOU.

   b. If you retire, transfer, or leave the organization,, you must notify the dSOs, return your smartcard to them for deactivation, and sign a Log Sheet for Deactivated Smartcards.

   c. Think of your smartcard as a personal credit card or blank check. The Electronic Signature generated by the smartcard is your signature. If another person uses it, you will bear the consequences.

4. SECURITY OF YOUR SMARTCARD AND PIN. A lost smartcard or compromised PIN is a serious security issue. You can be held responsible for transactions authorized with the missing or compromised card.

   a. If your PIN is revealed to someone else or you suspect it has been compromised, contact a dSO immediately for a new smartcard. Take the smartcard to the dSOs for deactivation and sign the Log Sheet for Deactivated Smartcards. Messages previously "signed" by you may still be verified.

   b. If your smartcard is lost/stolen, contact a dSO immediately for deactivation. You must go to the dSOs to obtain a new smartcard and PIN and sign a Log Sheet for Lost/Stolen Smartcards. Signatures generated by the lost/stolen smartcard after the deactivation date may not be verified.

5. SECURITY VIOLATIONS - WHAT SHOULD YOU REPORT? In addition to the above, report the following to the Security Office.

   a. If you see or know of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual’s supervisor for appropriate disciplinary action.

   b. If you find an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If you cannot log them off, remove the smartcard and take to the individual’s supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

c. If you find a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

d. If you find a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.

I certify that I have read and understand my responsibilities as a Smartcard Holder and that I am a Government employee.

PRINTED OR TYPED NAME **SIGNATURE**

OFFICE SYMBOL **EXTENSION** **DATE**

APPENDIX B

SMARTCARD APPROVERS DUTIES

APPENDIX B

SMARTCARD APPROVERS DUTIES

1. Each Corps of Engineers Financial Management System (CEFMS) site must appoint at least one Smartcard Approver. Smartcard Approvers will be appointed in writing and will be responsible for approving smartcard requests from Users and Security Administrators (SAs).

2. Smartcard Approvers will ensure the smartcard requestor is a Government employee. If in doubt, call the Security Office.

3. The Smartcard Approver must have a UNIX user ID and password and be given authority in the CEFMS Access Control Table to approve smartcard requests. Each Smartcard Approver must have a smartcard and PIN in order to electronically approve the requests.

4. A REQUEST FOR CEFMS ACCESS FORM must be completed for **each** employee requiring access to the CEFMS database. The forms will be submitted to the CEFMS DataBase Administrator. The CEFMS DBA will ensure the appropriate Smartcard Approver receives the names of individuals needing a smartcard.

5. Employees needing a smartcard will enter the CEFMS database and request a smartcard. The smartcard request will be forwarded electronically to the Smartcard Approver for action.

6. The Smartcard Approver must approve or disapprove the request. The APPROVE ELECTRONIC SIGNATURE SMARTCARD REQUEST SCREEN provides this capability. Access to this screen is limited to personnel designated as Smartcard Approvers.

   a. The APPROVE ELECTRONIC SIGNATURE SMARTCARD REQUEST screen displays all the smartcard requests that have not been approved or disapproved. The Smartcard Approver may use the arrow keys to scroll up and down through the pending requests. The cursor will automatically be positioned in the approved field for each pending request as they are scrolled.

   b. A request may be approved by entering "Y" or disapproved by entering "N" in the approved field.

c. If the Smartcard Approver desires, the <PgDn> key may be depressed to display detailed information about the request. To exit this screen, depress <Enter> to return to the original APPROVE/REJECT SMARTCARD REQUEST SCREEN.

d. When the Smartcard Approver is finished approving smartcard requests, depress the <End> key to commit the requests. If you depress the <F10> key, the screen will be exited and all approval actions will be discarded.

e. The approvals will be forwarded electronically to the dSOs who will issue the materials and PIN envelopes.

I certify that I have read and understand my responsibilities as a Smartcard Approver.

PRINTED OR TYPED NAME

SIGNATURE

OFFICE SYMBOL

EXTENSION

DATE

APPENDIX C

DISTRICT SECURITY OFFICER (dSO)

OPERATING PROCEDURES

APPENDIX C

DISTRICT SECURITY OFFICER (DSO) OPERATING PROCEDURES

1. Designation of dSOs and Responsibilities.

   a. Each Corps of Engineers Financial Management System (CEFMS) site will have two primary dSOs designated dSO1 and dSO2 to perform Electronic Signature management functions for smartcards. DSO1 and dSO2 must have at least one backup (but no more than two) to perform their same functions. The backups are designated dSOb1 and dSOb2. **If a primary dSO and backup are both absent, Electronic Signature functions can not be performed.**

      (1) DSO1 (and dSOb1) will be responsible for the security and issuing of User smartcards and Security Administrator (SA) Personal Identification Number (PIN) envelopes.

      (2) DSO2 (and dSOb2) will be responsible for the security and issuing of SA smartcards and User PIN envelopes.

   b. Each dSO and backup will have a UNIX user ID and password and will be granted privileges by the CEFMS DataBase Administrator (DBA) to perform dSO functions. These functions will be set in the CEFMS Access Control Table.

   c. DSOs will be appointed in writing, must be government employees, and given training in the operating procedures and security requirements for Electronic Signatures before performing dSO functions.

   d. Smartcard Holders will be valid CEFMS users and have assigned authorization for electronic signature capability. DSOs will verify an individual's status before assigning, activating, or issuing a Smartcard. If unsure, dSOs will contact the Security Office.

Reference the dSO Manual for additional responsibilities and operating procedures.